iDEFENSE

VeriSign

// THE POWER OF INTELLIGENCE

Internet Explorer Vulnerabilities and Malicious Code

An iDEFENSE Security Report
iDEFENSE Intelligence Operations

Sept. 1, 2005

Table of Contents

Copyright 2005 iDEFENSE Inc.
iDEFENSE is a VeriSign Company

1 Executive Summary

The Internet Explorer (IE) Web browser has existed for approximately 10 years, and became widely popularized in the late 1990s when it was packaged with Microsoft Corp.'s Windows operating systems. The fact that many companies have developed large Web application suites around IE has also contributed to its current widespread use and prevalence. However, as online security becomes more important and visible, many users have begun switching to other browsers that claim to offer greater default security measures. Despite the availability of competitor browsers, however, IE still commands 88.86 percent of the market share[1]; this is especially true in enterprise settings.

While most software packages contain some number of inherent exploitable vulnerabilities, very few have been as specifically targeted by attacks as IE. The number of Trojan horses, viruses, worms, phishing attacks, and spyware and adware applications that have specifically targeted this application in the last few years is staggering. The objective of this report is to analyze the IE components that have been targeted by malicious code in the past, and from that historical knowledge derive a sense of future trends.

[1] http://www.websidestory.com/products/web-analytics/datainsights/spotlight/05-10-2005.html

Copyright 2005 iDEFENSE Inc.
iDEFENSE is a VeriSign Company

2 History of Internet Explorer

IE 1.0 was the first Web browser introduced by Microsoft in July 1995. It was primitive in comparison to its present version, and was only available for Windows 95.

IE 2.0 was released in November 1995 for both Windows and Macintosh; it boasted some major additions, including support for SSL (HTTPS), HTTP Cookies and a Virtual Reality Modeling Language.

IE 3.0 was released in August 1996 for Windows NT 4, 95 and 98. Its most notable additions were Cascading Style Sheets (CSS), media file support (JPG, GIF, MIDI) and support for frames. It was with the release of IE 3.0 that vulnerabilities began to appear, including a frame spoofing vulnerability and a vulnerability that allowed access to a non-existent SMB share. Exploitation of this vulnerability automatically transmitted the username and encrypted password of the vulnerable computer to a predefined website. Another vulnerability allowed an attacker to launch commands via the DOS command line. The emergence of these vulnerabilities ushered in an era of failed patching, during which several IE vulnerabilities that should have been fixed reemerged.

The release of IE 4.0 in 1997 added more functionality, including DHTML and an Outlook Express 4.0 component. As with IE 3.0, vulnerabilities in 4.0 surfaced in large numbers. In 1997 and 1998, the BugTraq mailing list was filled with messages about IE 4.0 vulnerabilities.

IE 5.0 was released in 1998 and was first version to incorporate Internet security zones. This was a landmark event since it was a new feature specifically introduced to protect users. Unfortunately, the effectiveness of the zone model came into question when several vulnerabilities that caused cross-domain attacks were found. IE 5.0, although somewhat dated, is still widely used today and continues to be plagued by vulnerabilities. At the time of this writing, IE 6.0 is the most recent, stable version of IE and the most popular browser on the Internet.

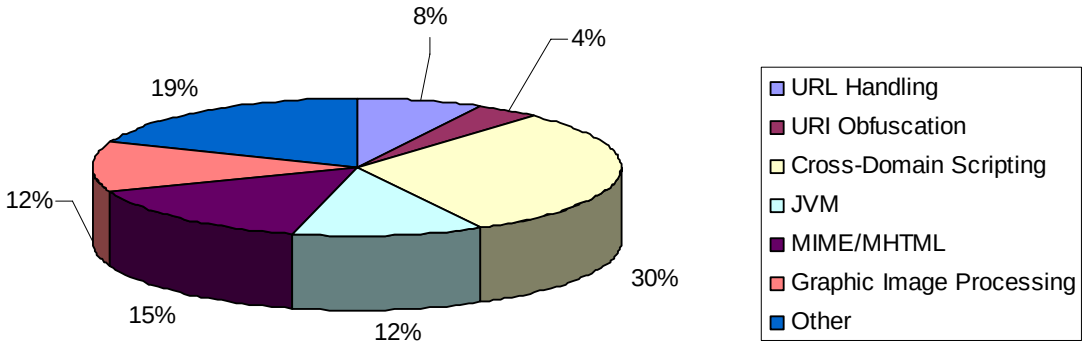
Copyright 2005 iDEFENSE Inc.
iDEFENSE is a VeriSign Company

3 Statistics and Trends in Malicious Code Targeting IE

To determine whether an application is truly secure, several statistics must be analyzed. In the case of IE, the number of vulnerabilities alone means very little in terms of overall security. For example, IE contains a large number of vulnerabilities that cause denial of service (DoS) conditions, which could lead to browser crashes. While important from a reliability perspective, these types of vulnerabilities are seldom exploited by malicious code. In the scope of malicious code exploitation, the most important browser vulnerabilities are those that lead to the arbitrary code execution or alter IE's security settings. While reviewing data compiled by iDEFENSE on IE exploitation by malicious code, it quickly became apparent that the following six areas were primarily being targeted:

- URL Handling
- URI Obfuscation
- Cross-Domain Scripting
- JVM
- MIME/MHTML Handling
- Graphic Image Processing

Vulnerabilities Exploited by Malicious Code per Area



Copyright 2005 iDEFENSE Inc.
iDEFENSE is a VeriSign Company

3.1 Common Areas of Exploitation

To understand how malicious code may target an application, one must first determine which areas of the application may be vulnerable. It is also important, especially in the case of IE, to understand the tight integration between this program and other Microsoft applications, most notably Outlook. This integration has resulted in a several vulnerabilities that can span multiple applications and which, in many cases, share the same code components. One of the most important areas of exploitation is processing and displaying MIME and HTML content, as IE, Outlook and other Microsoft applications share this functionality. Such functionality re-use creates a target-rich environment for malicious code that benefits from the fact that users must patch and lock down multiple applications to completely mitigate a threat. The following sections discuss the main areas of IE that have been exploited by malicious code. All of the vulnerabilities referenced in these tables with MS Security Bulletin numbers have been patched. Some of the minor issues have no security bulletin, indicating that they have either been left unpatched because they are of low priority, or have been patched as part of another vulnerability patch.

3.1.1 Cross-Domain Scripting Vulnerabilities

Design errors leading to cross-domain scripting are the most widely exploited vulnerabilities within IE. To date, there have been dozens of vulnerabilities that break the domain model protection scheme in this application. Only a small percentage, however, are actually exploited by malicious code, since many of the cross-domain vulnerabilities only allow JavaScript to be executed in the Local Zone. This usually limits attackers to stealing cookies or executing known programs without permission. The most widely recognized exploitation of these vulnerabilities types is through the use of iFRAME. This exploitation typically involves an attacker making a Web page that contains an iFRAME in which one Local Zone website is loaded through the iFRAME. This page then exploits a vulnerability that permits the parent frame to inherit its properties, changing its security settings, which then allows it to open in the Local Zone. As benign as these Local Zone JavaScript execution vulnerabilities seem, they can have damaging consequences when exploited in conjunction with other IE vulnerabilities that allow files to be placed on the hard drive of the computer running IE. An example of this kind of combined exploitation was the Bizex.A (ID# 208899, May 23, 2005) Trojan horse, which exploited the "Microsoft IE 6.0 showhelp() CHM XSS Vulnerability" (ID# 210843, Oct. 12, 2004) and the "Microsoft Java Virtual Machine Bytecode Verifier Design Error" (ID# 303210, April 9, 2003).

The following chart illustrates the cross-domain vulnerabilities in IE:

ID#	Vulnerability Name	Type	Versions	ActiveX	MS Number	Date
302096	Microsoft XML Core Services XMLHTTP Information Disclosure Vulnerability	Cross-Domain	6	Yes	MS02-008	2/21/2002
303386	Microsoft Internet Explorer JS/DragDrop Vulnerability	Cross-Domain	5.01,5.5,6,6SP1	Yes	MS03-015	4/23/2003
205836	Microsoft IE Object Tag XML Data Binding Vulnerability	Cross-Domain	5.01,5.5,6,6SP1	Yes	MS03-040	9/10/2003
303396	Microsoft Internet Explorer IFRAME vulnerability	Cross-Domain	6, 6 SP1	Yes	MS03-020	5/9/2004
211449	Microsoft IE showModalDialog HTTP Redirection Vulnerability	Cross-Domain	5.5,6, 6 SP1	Yes	MS04-025	6/7/2004

Copyright 2005 iDEFENSE Inc.
iDEFENSE is a VeriSign Company

401732	Microsoft Internet Explorer Drag-And-Drop STYLE Vulnerability	Cross-Domain	5.01,5.5,6,6SP1	Yes	MS04-038	8/21/2004
210843	Microsoft IE 6.0 showhelp() CHM XSS Vulnerability	Cross-Domain	6, 6 SP1	No		10/12/2004
404589	Microsoft IE hhctrl.ocx Help ActiveX Control Local Zone Security Restriction Bypass Vulnerability	Cross-Domain	6, 6 SP1	Yes	MS05-001	10/20/2004

3.1.2 MHTML and MIME-Related Vulnerabilities

MIME and MHTML vulnerabilities affect content using MIME extensions, which is most popular in e-mail systems. When exploited, these vulnerabilities often result in arbitrary code or script execution. These vulnerabilities are commonly targeted because they can usually be exploited through IE and e-mail clients, such as Outlook and Outlook Express, using IE for parsing and displaying HTML content. There have been several malicious codes targeting these types of vulnerabilities in IE, most notably variants of the NetSky, BugBear and Aliz worm families.

In terms of severity, these vulnerabilities can rate very high since they lead directly to the arbitrary code execution and require little or no user interaction to execute the downloaded code. Furthermore, unlike other IE vulnerabilities that are used in conjunction with techniques or other vulnerabilities that lower the browser's security settings, MIME and MHTML vulnerabilities are mostly standalone. The following table is a summary of the IE MIME and MHTML vulnerabilities exploited by malicious code:

ID#	Vulnerability Name	Type	Versions	ActiveX	MS Number	Date
301564	Microsoft Internet Explorer 5 MIME Attachment Execution Vulnerability	MIME	5.01, 5.5	No	MS01-020	3/29/2001
302871	Microsoft Outlook Script Execution Vulnerability	MHTML, URL Handler	5.5, 6	No	MS03-014	12/14/2002
207012	Microsoft Internet Explorer MHTML Download and Execution XSS Vulnerability	MHTML	6, 6 SP1	No		11/25/2003

3.1.3 URI-Obfuscation Vulnerabilities

Uniform Resource Identifier (URI) obfuscation vulnerabilities allow malicious code to be successfully downloaded to a computer by hiding its original destination and masquerading as a known and trusted website. This obfuscation can occur as a result of how the browser processes and displays different character sets and/or HTML tags. These vulnerabilities have been widely used in malicious code and phishing website attacks.

ID#	Vulnerability Name	Type	Versions	ActiveX	MS Number	Date
207304	Microsoft IE Address Bar URI Display Obfuscation Vulnerability	URI Obfuscation	5.01, 5.5, 6, 6SP1	No	MS04-004	12/17/2003

Copyright 2005 iDEFENSE Inc.
iDEFENSE is a VeriSign Company

3.1.4 Microsoft Java Virtual Machine Vulnerabilities

Vulnerabilities in Microsoft's Java Virtual Machine make up a considerable percentage of the publicly disclosed vulnerabilities in IE. Despite this, a significantly small percentage of these vulnerabilities have had public exploit code released, and an even smaller portion of these have been exploited by malicious code.

A very important factor mitigating the threat posed by these vulnerabilities is that Microsoft no longer distributes the JVM. Microsoft also formally announced that the MSJVM support lifecycle will end on Dec. 31, 2007. In spite of this, malicious code targeting the MSJVM continues meet with success since there are many legacy applications that still require this IE component. One recent example is the JevProx.A Trojan horse (ID# 416835, July 18, 2005), which successfully exploited the MS05-037 "Microsoft IE JVIEW Profiler (Javaprxy.dll) Heap Overflow Vulnerability" in several very large enterprise environments where the MSJVM was used to support legacy applications.

ID#	Vulnerability Name	Type	Versions	ActiveX	MS Number	Date
301228	Microsoft Virtual Machine Access Validation Vulnerability	JVM	4,5,5.01	No	MS00-075	12/21/2000
303210	Microsoft Java Virtual Machine Bytecode Verifier Design Error	JVM	4, 5, 5.5	No	MS03-011	4/9/2003
414992	Microsoft IE JVIEW Profiler (Javaprxy.dll) Heap Overflow Vulnerability	JVM	5.01, 5.5, 6, 6 SP1	No	MS05-037	6/30/2005

3.1.5 URL-Handling Vulnerabilities

URL Handling vulnerabilities compose a small percentage of the total number of vulnerabilities found in IE, and a small percentage of the actual number of vulnerabilities exploited by malicious code. While the total number of vulnerabilities that exploit the URL handler vulnerability is small, the number of malicious codes that have exploited these vulnerabilities is substantial. According to data contained in the iDEFENSE malicious code database, the MS-ITS URL Handler vulnerability is the second most widely exploited IE vulnerability. Most notable of the codes that exploit URL vulnerabilities is the Ibiza.A (ID# 208697, Feb. 12, 2004), which targeted the "Microsoft Internet Explorer/Outlook Express MS-ITS URL Handler Vulnerability (iDEFENSE Exclusive)" (ID# 208704, Jan. 2, 2004). This particular malicious code incident is of importance since this code appeared seven days before a patch was released. The following table illustrates the IE URL Handling vulnerabilities that have been exploited by malicious code.

ID#	Vulnerability Name	Type	Versions	ActiveX	MS Number	Date
302871	Microsoft Outlook Script Execution Vulnerability	MHTML, URL Handler	5.5,6	No	MS03-014	12/14/2002
208704	Microsoft Internet Explorer/Outlook Express MS-ITS URL Handler Vulnerability (iDEFENSE Exclusive)	URL Handler	5, 5.01, 5.5,6,6 SP1	No	MS04-013	1/2/2004

Copyright 2005 iDEFENSE Inc.
iDEFENSE is a VeriSign Company

3.1.6 Image Processing Vulnerabilities

Image processing vulnerabilities are, for the most part, a new area of exploitation not only in IE but also in the Windows operating system altogether. These vulnerabilities are usually the result of how an application handles specific malformed images and often lead to arbitrary code execution. This particular type of vulnerability, although not heavily exploited by malicious code, could be used as an effective means of propagation. Because of the way image handling components are often shared in the Windows operating system, these vulnerabilities are difficult to mitigate without a vendor patch, since disabling them would greatly reduce IE's (and perhaps even the entire operating system's) functionality and usability. Most notable of the malicious code targeting these types of vulnerabilities are the BMPAgent.A (ID# 210869, May 14, 2004) and the Anicmoo.A (ID# 407292, Feb. 16, 2005) Trojan horses. BMPAgent.A is another example of a Trojan horse that exploited a vulnerability 77 days before a patch was released. The following table outlines the image processing vulnerabilities in IE:

ID#	Vulnerability Name	Type	Versions	ActiveX	MS Number	Date
208745	Microsoft Internet Explorer 5.x/6.0 Bitmap Image Integer Overflow Vulnerability	Image	5, 5.01, 5.5,6,6 SP1	No	MS04-025	2/15/2004
402456	Microsoft Multiple Application/OS GDI+ JPEG Processing Buffer Overflow Vulnerability	Image	6, 6 SP1	No	MS04-028	9/14/2004
405948	Microsoft Windows Cursor, Icon Format Handling Vulnerability	Image	5.01, 5.5, 6, 6 SP1	No	MS05-002	1/11/2005

3.1.7 Other Design Error Vulnerabilities

There are several other areas of IE that contain vulnerabilities that have been exploited by malicious code. Most important among these areas are the handling of certain object types and the processing and authentication of ActiveX. According to the data contained in the iDEFENSE malicious code database, the "Microsoft Internet Explorer 6.x ADODB.Stream Object Vulnerability" (ID# 205330, Aug. 26, 2003) is the most exploited IE vulnerability ever, with more than 150 malicious codes designed to exploit it. This vulnerability was initially documented by iDEFENSE as being used by infected spam e-mails (ID# 206780, Nov. 13, 2003). Another malicious code that targeted this vulnerability was the Scob Trojan horse (ID# 400157, July 2, 2004). The following table summarizes of these "other" areas that have been exploited by malicious code in IE:

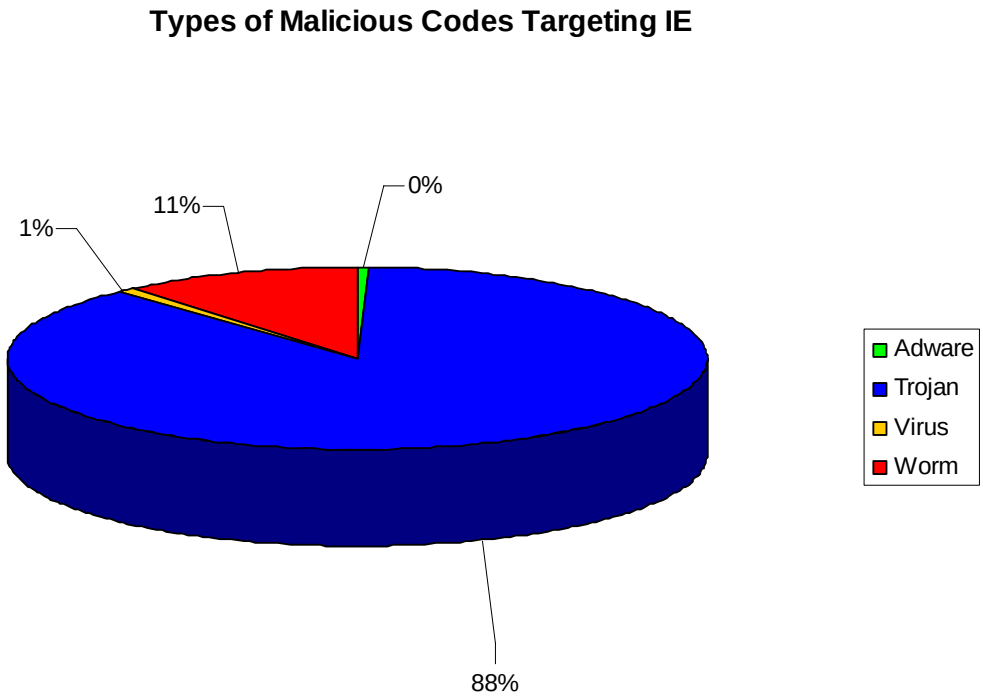
ID#	Vulnerability Name	Type	Versions	ActiveX	MS Number	Date
204989	Microsoft IE Object Type Buffer Overflow in Double-Byte Character Set Environment	Other Design	5.01,5.5,6,6SP1	Yes	MS03-032	8/26/2003
205330	Microsoft Internet Explorer 6.x ADODB.Stream Object Vulnerability	Other Design	5.5,6, 6 SP1	Yes	MS03-048	8/26/2003

Copyright 2005 iDEFENSE Inc.
iDEFENSE is a VeriSign Company

206165	Microsoft Authenticode ActiveX Verification Vulnerability	Other Design	5.01,5.5,6,6SP1	Yes	MS03-041	10/15/2003
300577	Microsoft Internet Explorer 5.x Active X Controls Access Validation Error	Other Design	4, 5,5.01	Yes	MS99-032	8/31/1999
302377	Microsoft Internet Explorer Local File Script Design Vulnerability	Other Design	5.5,6	No	MS02-015	3/28/2002
403553	Microsoft Internet Explorer Malformed IFRAME Remote Buffer Overflow Vulnerability	Other Design	6 SP1	No	MS04-040	10/27/2004

3.2 Types of Malicious Code Targeting IE

At the time of this writing, there are more than 433 reported malicious codes targeting IE vulnerabilities. These malicious codes can be broken down into several different categories, and most recently spyware and adware have begun to exploit IE vulnerabilities to infect an unsuspecting user's computer. It must be noted that, although a large number of spyware is delivered via IE, only a small number is currently performing actual exploitation. Most commonly, spyware is installed though social engineering techniques, bundled with a legitimate software package or dropped by a malicious code that performs the initial exploitation. The following graph shows the percentage of each malicious code type targeting IE:

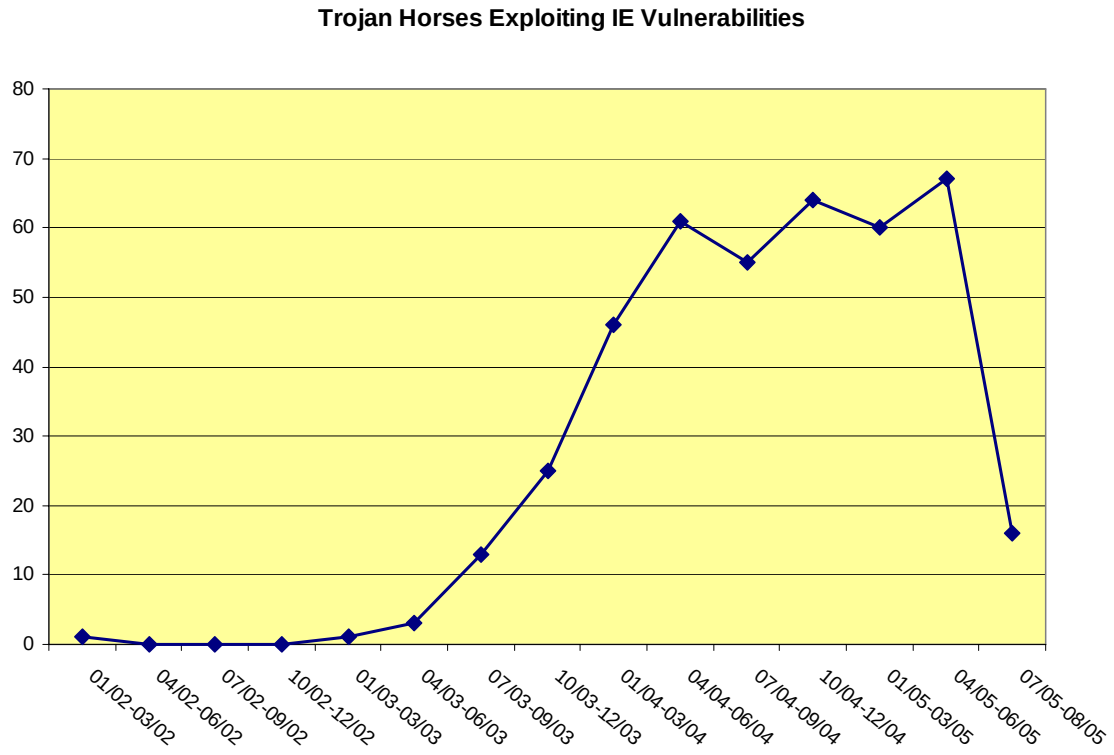


Copyright 2005 iDEFENSE Inc.
iDEFENSE is a VeriSign Company

A search of the iDEFENSE malicious code database reveals that the majority of the malicious codes targeting IE are Trojan horses, the majority of which are "droppers" that download and execute other codes. These downloaded codes can include worms, viruses, and adware and spyware applications. Several of these Trojan horses also modify IE settings or other network traffic routing mechanisms such as DNS tables, hosts files, browser start pages and browser helper objects to direct users to websites chosen by the malicious actor.

Many of these Trojan horses are used for monetary gain, and these types of attack usually lead to the unintended disclosure of information or the display of unwanted advertisements. In some cases, these Trojan horses create backdoors on the infected computer that could allow remote access. These backdoors are generally used for stealing information, setting up proxy servers for use in spam or phishing scams, and carrying out distributed denial of service (DDoS) attacks.

The number of malicious codes released that target IE vulnerabilities can be directly linked to the discovery and public disclosure of vulnerabilities. The following chart examines the number of Trojans horses released for IE over the last three years. There are noticeable spikes when vulnerabilities with public exploit code emerge. Notice how the graph spikes when it was discovered that the "Microsoft Internet Explorer 6.x ADODB.Stream Object Vulnerability" (ID# 205330, Aug. 26, 2003) patch was insufficient in late 2003. During this time, several attacks against IE occurred, including the Scob Trojan horse (ID# 400157, July 2, 2004) and more than 100 Psyme Trojan horse family variants. In the third quarter of 2004, a similar pattern was observed after the public disclosure of the "Microsoft Multiple Application/OS GDI+ JPEG Processing Buffer Overflow Vulnerability" (ID# 402456, Sept. 14, 2004) . Yet again in the first two quarters of 2005, similar spikes in the number of Trojan horses targeting IE were seen after the public disclosure of the "Microsoft IE hhctrl.ocx Help ActiveX Control Local Zone Security Restriction Bypass Vulnerability" (ID# 404589, Oct. 20, 2004).



Copyright 2005 iDEFENSE Inc.
iDEFENSE is a VeriSign Company

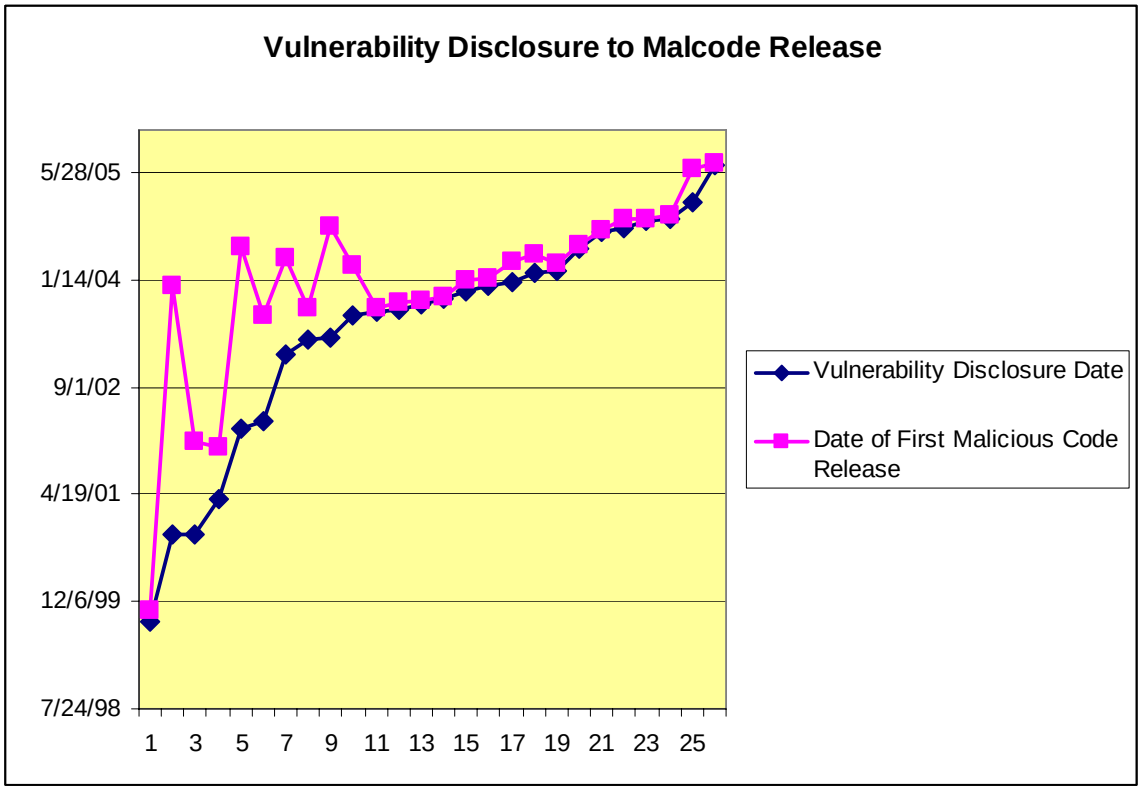
3.3 Malicious Code vs. Vulnerability Patch Time

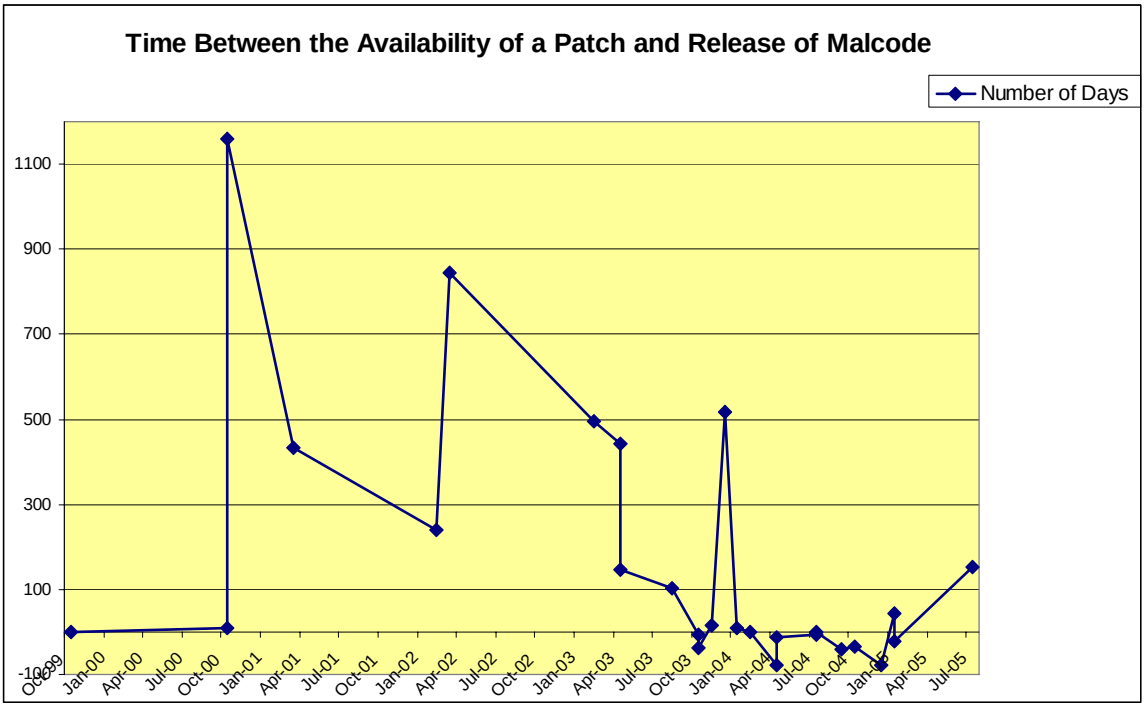
Most malicious code targeting IE, although potentially serious, has targeted vulnerabilities for which patches were available. For a very long time, malicious code targeted vulnerabilities patched for at least one year, such as the "MIME Attachment Vulnerability" (ID# 301564, March 29, 2001) and the "Virtual Machine Access Validation Vulnerability" (ID# 301228, Dec. 21, 2001). One of the major turning points in malicious code targeting IE occurred in 2003 when the ADODB Stream Vulnerability MS03-048 was released. The first malicious code to exploit this vulnerability emerged after the MS03-048 advisory. However, the first patch released did not work properly, resulting in a series of malicious codes being released that exploited the unpatched IE instance. To date, this has been one of the largest exploitations of IE, resulting in, as previously stated, more than 150 instances of exploitation.

The ADODB vulnerability was not the last of the unpatched vulnerabilities. In February 2004, the "Microsoft Internet Explorer/Outlook Express MS-ITS URL Handler Vulnerability (iDEFENSE Exclusive)" (ID# 208704, Jan. 2, 2004) was exploited. iDEFENSE customers had 45 days to implement a workaround between the time the vulnerability was disclosed and the appearance of the first malicious code. When the first malicious code was released, there were still 57 days before Microsoft released a patch. Even after the patch was released, this vulnerability remained a popular choice for malicious code writers. Both websites in the Widespread DNS Poisoning Incident of 2005 (ID# 409855, April 8, 2005) and the TGP.la (ID# 411772, May 9, 2005) incident contained malicious code that installed Trojans by exploiting this vulnerability. Another successful piece of malicious code that exploited this vulnerability was the Scob Trojan horse (ID# 400157, July 2, 2004). Scob was one of the most important IE malicious code incidents, even though it was part of a multi-stage attack in which attackers placed the Trojan on hacked IIS Web servers to infect visitors. According to research performed by the iDEFENSE Malicious Code Team, this attack was conducted by members of a well-know hacker group who used it to compromise systems worldwide.

An analysis of data gathered by iDEFENSE (below) on both malicious code and IE vulnerabilities clearly indicates that the time between public disclosure of a vulnerability and the appearance of malicious code in the wild has diminished over IE's lifetime. This timeframe has been reduced from a few months to only weeks, and, in some cases, days. In the most recent exploitation of the "IE COM Object Instantiation Memory Corruption Vulnerability" (ID# 418970, Aug. 12, 2005) the time between disclosure and the appearance of malicious code was only six days. This is a disturbing trend that clearly highlights the importance of patching vulnerable systems in the most expedient manner possible. This same data set also reveals that the time between the availability of a patch and the appearance of malicious code in the wild is diminishing for IE. This development can have serious consequences, especially if there is no feasible workaround, since users have little or no protection. It is also worth mentioning that iDEFENSE has documented the existence of 42 unpatched IE vulnerabilities at the time of this writing.

Copyright 2005 iDEFENSE Inc.
iDEFENSE is a VeriSign Company





Copyright 2005 iDEFENSE Inc.
iDEFENSE is a VeriSign Company

4 Case Studies

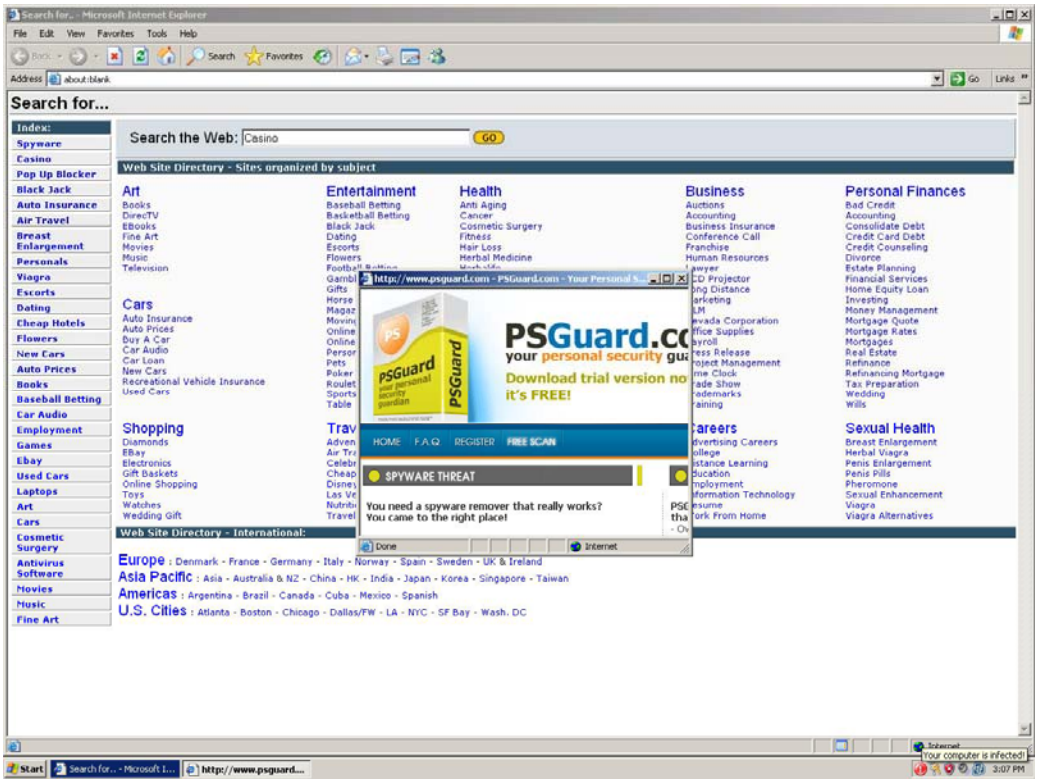
4.1 Lab Test 1 - Windows XP SP2 - IE 6 Default Settings

For this lab test, the following system was used:

Operating System: Windows XP Pro (SP2)
Browser: Internet Explorer 6 - Default Security Zone (MEDIUM)

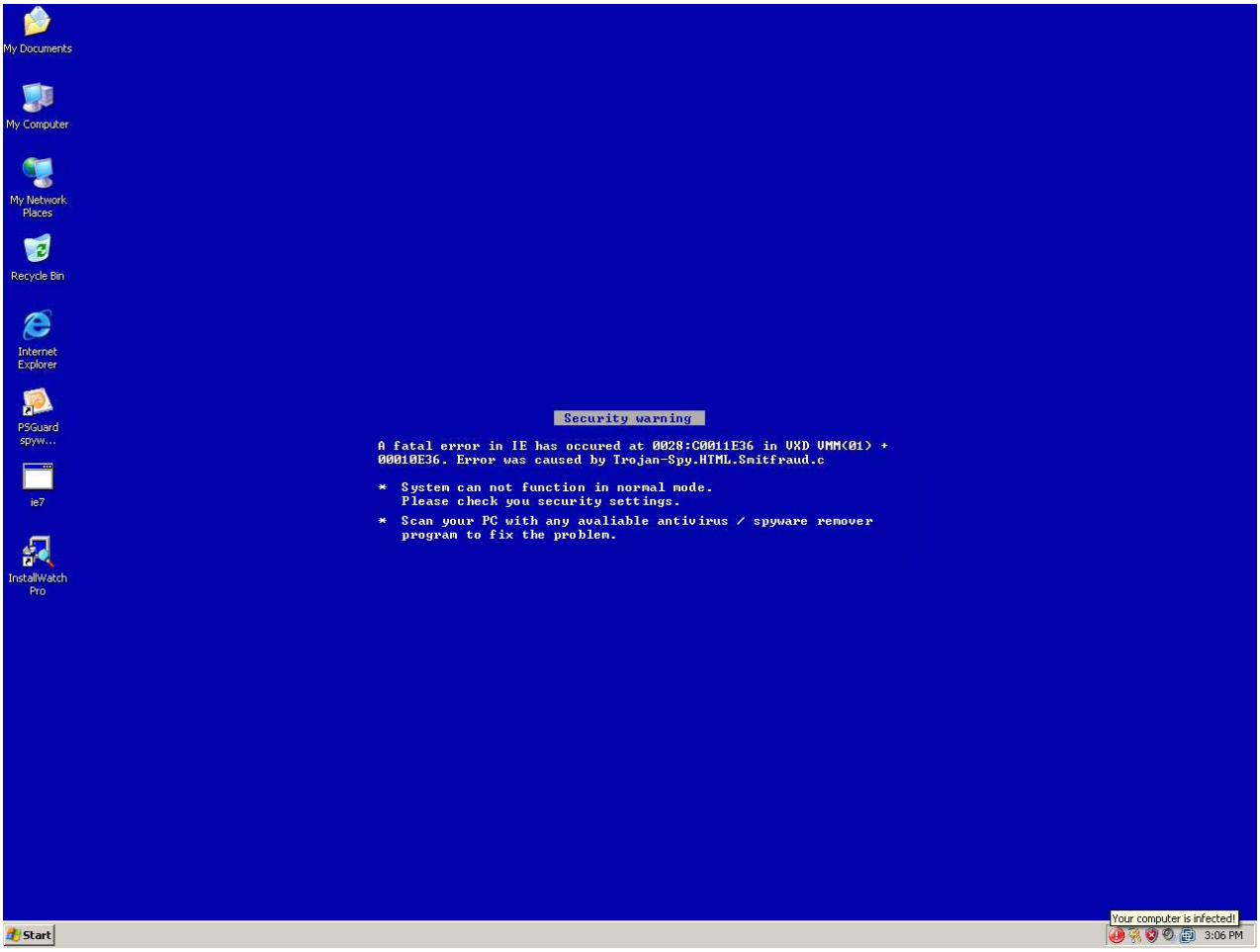
Internet Explorer 6 for XP SP2 is the most up-to-date version of Internet Explorer and includes many new features and fixes not available for Windows 2000. In conducting this lab test, it was assumed that, under the default settings, the browser would be secure as long as no human interaction (e.g., clicking "accept" or "yes") occurred. Installation monitoring software was installed to record all changes and then rigorous website surfing was started. For the purpose of these tests, iDEFENSE analysts visited many websites known to contain malicious content. While this may not always accurately represent how a corporate user browses the Internet, it does show the potential for harm when malicious websites are accessed, whether intentionally or not.

What was most striking about the test is that even without any user interaction, with the exception of hitting "no" or "cancel" in response to various messages that appeared during testing, the iDEFENSE lab server was infected by malicious codes within 15 minutes of Web surfing. One of the codes installed on the test computer was the Alemod.D (ID# 416487, Aug. 3, 2005) Trojan horse, which infected the test computer within minutes. This infection led to the display of a small icon claiming the computer was infected with spyware:



Copyright 2005 iDEFENSE Inc.
iDEFENSE is a VeriSign Company

The background of the computer was also changed to a message attempting to trick a user into running the spyware tool, which now appeared in the taskbar. The icon was clicked, representing the first instance of user interaction associated with these lab tests. After clicking the icon, the malicious code downloaded more files from a website and made additional Windows registry changes. The following screenshot shows what is displayed when IE is launched after clicking the icon:



After 15 minutes of surfing known infected websites with a fully patched IE 6.0 Web browser, a total of 36 files were downloaded to the computer's hard drive. Most of them were actually part of the temporary Internet files and would simply be removed when the browser cache was cleared. Unfortunately, there were also several malicious code files dropped into the Windows System directory that would not be removed when the browser cache was cleared.

There were four .ini files found in the temporary Internet files that referenced changes to the desktop.ini settings (i.e., changes to the desktop wallpaper):

- C:\Documents and Settings\aaron\Local Settings\Temporary Internet Files\Content.IE5\FNYIATAZ\desktop.ini,.ShellClassInfo,UICLSID,{7BD29E00-76C1-11CF-9DD0-00A0C9034933}

Copyright 2005 iDEFENSE Inc.
iDEFENSE is a VeriSign Company

- C:\Documents and Settings\aaron\Local Settings\Temporary Internet Files\Content.IE5\O64G5N3G\desktop.ini,.ShellClassInfo,UICLSID,{7BD29E00-76C1-11CF-9DD0-00A0C9034933}

- C:\Documents and Settings\aaron\Local Settings\Temporary Internet Files\Content.IE5\QF4YNNJ1\desktop.ini,.ShellClassInfo,UICLSID,{7BD29E00-76C1-11CF-9DD0-00A0C9034933}

- C:\Documents and Settings\aaron\Local Settings\Temporary Internet Files\Content.IE5\SDDB2NER\desktop.ini,.ShellClassInfo,UICLSID,{7BD29E00-76C1-11CF-9DD0-00A0C9034933}

The most shocking test result was the number of Windows registry changes. There were 120 Windows registry entries added or changed as a result of the 15 minutes of website surfing. Due to their length, they will not be included in this report; there were, however, various changes in Internet Explorer settings, desktop settings, startup settings and connection settings.

4.2 Lab Test 2 - Windows XP SP2 - IE 7 Beta Default Settings

For this lab test, the following system was used:

Operating System: Windows XP Pro (SP2)
Browser: Internet Explorer 7 Beta

After accessing known malicious websites for more than 30 minutes using IE 7, no files were downloaded to the test system, nor were any Windows registry entries created or changed. Although it is good that no known exploitation techniques from IE 6 were successful in IE 7, this does not mean that the browser is truly safer, only that it is safe from current threats. Until IE 7 is released and becomes widely adopted, there will be little reason for anyone to exploit it. As a result, these lab tests really only demonstrate that IE 5 and 6 exploit codes contained on known infected websites do not affect IE 7. During these lab tests, iDEFENSE found that one of the security features seemed to be inconsistent with the specification. The address bar was not always displayed when pop-up windows appeared. Instead, they appeared as they had in previous versions of IE, and actually made the browser freeze until they were closed. Even though IE 7 is still in the early beta stages, any divergence from the specification, especially when it comes to security features, should be closely monitored. Despite this issue, which can probably be attributed to the early stage of the software's development, Microsoft must be commended for fixing so many of the security features that have plagued IE over the last several years.

Copyright 2005 iDEFENSE Inc.
iDEFENSE is a VeriSign Company

5 The Future of IE

As long as IE is packaged with Windows operating systems, and as long as Windows remains popular, many users will continue to use this built-in browser. In determining the future of malicious code targeting IE, one must first examine future browser changes. Microsoft has released a technical paper detailing changes in the new IE 7[2]. This section examines each of the changes identified by Microsoft and how they affect malicious code.

5.1 URL-Handling Protection

Microsoft has rewritten URL handling so that only one function will handle all of the URLs from within the browser. If this feature is implemented properly, it will reduce the number of vulnerabilities and, in turn, reduce the number of malicious codes that are able to exploit such handling vulnerabilities. While the software may be more organized now, if a vulnerability were discovered in the handling function, it would have the exact same effect as in older versions. The difference now is that, if this occurs, the URL handler will only have to be fixed in one place, reducing patch time and the likelihood that it will be patched.

5.2 URL-Display Protection

One helpful feature that has been added to the beta 1 version is an address bar to all windows, including pop-up windows. While not in the beta 1, the Microsoft white paper states that more display control tools will be added to IE 7. This feature is extremely helpful and will definitely mitigate future malicious code attacks in this area if implemented correctly.

5.3 Cross-Domain Attack Protection

Cross-domain attacks present one of the largest vulnerability threats in IE. IE 7 is supposed to have a newly redesigned model that appends the domain of origin to each script so that it may only access its own items within its own domain. If this feature is implemented without design flaws, it will stop a large area of vulnerability exploitation.

5.4 Protected Mode

A "protected mode," which strips the browser of any privileges, is supposed to be added in the next IE 7 beta release. As a result, all communication will be completed through a broker process. Since this feature has not yet been examined by iDEFENSE, it is impossible to predict how well it works. If it works properly, it will mitigate many malicious codes that attempt to inject threads into or illegally use the IE process.

5.5 Phishing Filter

Microsoft is introducing a phishing filter to help track and stop phishing attacks. This is a useful and very welcomed feature that should make life very difficult for phishers. In the past, malicious code writers exploited not only browser vulnerabilities, but imitated browser features to trick users. It is very possible

[2] http://www.microsoft.com/downloads/details.aspx?FamilyId=718E9B3A-64FE-4A4C-9DDF-57AF0472EAD2&displaylang=en

Copyright 2005 iDEFENSE Inc.
iDEFENSE is a VeriSign Company

that this feature could be used in one of these social engineering attacks to trick a user into performing an action that will install malicious code.

5.6 Spyware

It is likely that the future will see more spyware and other malicious code exploitation of existing and new versions of IE vulnerabilities. These codes have become very prevalent in the last 18 months and have started to incorporate obfuscation techniques, making them extremely difficult to detect and remove. Many spyware codes are also undetectable by current anti-virus engines, a fact that further improves their chances of successfully infecting a computer.

Copyright 2005 iDEFENSE Inc.
iDEFENSE is a VeriSign Company

6 Mitigation Strategies

There are several strategies that organizations can employ to mitigate the threat of malicious code targeting IE. The first is to ensure that patches are applied to systems as soon as they are available. This greatly reduces the threat from most malicious codes targeting IE since most exploitation occurs against vulnerabilities for which a patch is available.

Another important mitigation strategy is to reduce the amount of active content that can be executed by IE. This measure also reduces the number of malicious codes that can be executed since most of the codes targeting IE use some form of active content like ActiveX or JavaScript.

Finally, restricting user privileges at the operating system level can effectively mitigate malicious code threats, since most codes will not be permitted to be installed to system directories for which the user has no write privileges, even when the browser is exploited. This situation is starting to change, however, since there are now several spyware codes that can install themselves on a user's machine even with very restricted privileges.

Vulnerabilities for which a patch does not exist will always be among the most dangerous for IE users. In this case, only knowledge of the vulnerability and the availability of a workaround are effective mitigation strategies.

Copyright 2005 iDEFENSE Inc.
iDEFENSE is a VeriSign Company

7 Conclusions

The problem of malicious code targeting IE is not going to go away until this browser becomes more difficult to exploit. Even then, unpatched systems and users with older IE versions will still be targeted by malicious code authors. In IE 5 and 6, the domain model, although a vast improvement in terms of security, still contains many vulnerabilities that are often exploited by malicious code. As important as these vulnerabilities are, they were dwarfed by the sheer number of exploitations resulting from the ADODB and MS-ITS URL Handling vulnerabilities. These incidents clearly demonstrate what can happen when a patch is unavailable or when it fails to properly correct a security flaw.

Microsoft has done an excellent job correcting problematic areas and introducing new security features in IE 7.0. This effort is testament to how seriously Microsoft is taking security in new versions of their product line. iDEFENSE lab test results are a testament to Microsoft's new version of IE and its attendant security features.

Copyright 2005 iDEFENSE Inc.
iDEFENSE is a VeriSign Company